WHAT IS CLAIMED IS:

1. A method of encrypting communications from a computer having an application program interface, the method comprising using a mobile communications device, which includes a cryptographic module for use in mobile communication, as a cryptographic service provider.

2. A method as claimed in claim 1, wherein the mobile communications device is a WAP-enabled device.

3. A method as claimed in claim 1, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

4. A method as claimed in claim 1, comprising providing a wired connection between the mobile communications device and the computer.

5. A method as claimed in claim 1, comprising providing a wireless connection between the mobile communications device and the computer.

6. A method as claimed in claim 1, comprising:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device.

7. A mobile communications device, comprising a cryptographic module, the cryptographic module being usable:

for encoding wireless communications from the device;

in a cryptographic service provider with an application program interface of a remote computer.

8. A mobile communications device as claimed in claim 7, having a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer.

9. A mobile communications device as claimed in claim 7, wherein the short-range wireless communications transceiver uses Bluetooth wireless technology.

10. A mobile communications device as claimed in claim 7, wherein the cryptographic module is usable to support wireless communications using Wireless Transport Layer Security.

11. A mobile communications device as claimed in claim 7, wherein the cryptographic module uses public key cryptography.

12. A mobile communications device as claimed in claim 7, comprising means for sending and transmitting data using WAP.

13. A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in hardware in the device.

14. A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in software in the device.

15. A mobile communications device as claimed in claim 7, wherein the cryptographic module is provided on an external smart card.

16. A mobile communications device as claimed in claim 7, wherein the cryptographic module comprises a Wireless Identity Module card.

17. A mobile communications device as claimed in claim 16, wherein the cryptographic module comprises a Wireless Identity Module card which allows communications using Wireless Transport Layer Security.

18. A mobile communications device as claimed in claim 7, comprising an interface for receiving a command from a personal computer, the mobile communications device acting as a cryptographic service provider for said personal computer in response to said command.

19. A module for a personal computer, wherein, in response to the module receiving a first command from a

cryptographic application program interface, indicating that it requires cryptographic functionality, the module sends a second command to a mobile communication device, such that the mobile communications device acts as a cryptographic service provider for said personal computer.

20. A method of encrypting computer communications, the method comprising using a separate mobile communications device, which includes a cryptographic module for use in mobile communication, as a cryptographic service provider.

21. A method as claimed in claim 20, wherein the mobile communications device is a WAP-enabled device.

22. A method as claimed in claim 20, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

23. A method as claimed in claim 20, comprising providing a wireless connection between the mobile communications device and the computer.

24. A computer system, comprising:

a computer; and

a mobile communications device, including a cryptographic module,

the computer having at least one application which requires cryptographic functionality,

a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device,

the computer and the mobile communications device having means for establishing a secure communications path therebetween; and

the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.

25. A computer system as claimed in claim 24, wherein the mobile communications device is a WAP-enabled device.

26. A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an internal memory access application.

27. A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an external communication application.

28. A method of providing cryptographic functionality in a computer having a cryptographic application program interface, the method comprising using a mobile communications device, which includes a cryptographic module for use in

mobile communication, to provide the cryptographic functionality.

29. A method as claimed in claim 28, wherein the mobile communications device is a WAP-enabled device.

30. A method as claimed in claim 28, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

31. A method as claimed in claim 28, comprising:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device.

32. A method as claimed in claim 28, comprising using a cryptographic module realized in hardware in the mobile communications device.

33. A method as claimed in claim 28, comprising using a cryptographic module realized in software in the mobile communications device.

34. A method as claimed in claim 28, comprising using a cryptographic module provided on an external smart card which can be read by the mobile communications device.

35. A method as claimed in claim 28, comprising using a cryptographic module provided on a Wireless Identity Module card in said mobile communications device.

36. A computer system for supporting an application, the computer system comprising:

a cryptographic application program interface; and

a cryptography service provider,

wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality, sends a command to the cryptography service provider, and

wherein the cryptography service provider has a communications link to a cryptographic module of a mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface, and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device.

37. A system as claimed in claim 36, wherein the cryptographic module is realized in hardware in the mobile communications device.

38. A system as claimed in claim 36, wherein the cryptographic module is realized in software in the mobile communications device.

39. A system as claimed in claim 36, wherein the cryptographic module is provided on an external smart card which can be read by the mobile communications device.

40. A system as claimed in claim 36, wherein the cryptographic module is provided on a Wireless Identity Module card in said mobile communications device.

41. A system as claimed in claim 36, wherein the cryptography service provider has a Bluetooth wireless communications link to the mobile communications device.

42. A system as claimed in claim 36, wherein the cryptography service provider has some cryptographic functionality, and, on receipt of a command from the cryptographic application program interface, determines whether it can perform the required cryptographic functionality, or whether to obtain the required cryptographic functionality from the cryptographic module of the mobile communications device.

43. A system as claimed in claim 36, wherein the communications link between the cryptography service provider and the cryptographic module of the mobile communications device uses a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

44. A mobile communications device, the mobile communications device being able to communicate over a first

wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface, the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second interface.

45. A mobile communications device as claimed in claim 44, wherein the security manager module responds to a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

46. A mobile communications device as claimed in claim 44, wherein the second interface is a Bluetooth short-range radio interface.

47. A module for a computer system, the module comprising:

an application interface for connection to a computer application; and

an external interface for connection to a mobile communication device containing a cryptographic module;

wherein, when the module receives from the application interface a request for a cryptographic function which the

module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom.

48. A module for a computer system as claimed in claim 47, wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested function cryptographic function.

49. A module for a computer system as claimed in claim 47, wherein the external interface is a Bluetooth short-range radio interface.

50. A module for a computer system as claimed in claim 47, wherein the module sends over the external interface a command from a command set as defined in a standard PKCS#11, where the commands are redefined as AT commands.